Privacy Impact Assessment Update
for the

Air Cargo Security Requirements

November 12, 2008

Contact Point

Victor Parker
Branch Chief, Policy and Strategic Planning, Air Cargo
Transportation Security Administration
(571) 227-3664

Reviewing Officials

Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Transportation Security Administration (TSA) is making several changes to its air cargo program that involve the collection of personally identifiable information (PII) and the addition of new populations for which information will be collected. First, for TSA conducted security threat assessments (STAs) on individuals participating in its air cargo programs, TSA is requiring the submittal of contact and employer information for all participants so TSA can contact the individual in the adjudication process. Second, TSA will allow non-citizens who do not have an Alien Registration Number to provide a Form I-94 Arrival/Departure number. Third, TSA is creating a new Certified Cargo Screening Program (CCSP), expanding the population of individuals who will need to provide PII for TSA-conducted STAs. A new automated collection STA Tool will be deployed to support the collection of PII from the CCSP population. Fourth, TSA is updating the records retention schedule and redress processes applicable to all populations submitting PII for STAs under its air cargo programs. In accordance with Section 222 of the Homeland Security Act of 2002, TSA is issuing this update (PIA Update) to the Air Cargo Security Requirements PIA published on April 14, 2006, to incorporate these changes. The April 14, 2006 PIA remains in effect to the extent that it is consistent with this update. This update should be read together with the 2006 PIA.

Introduction

Consistent with the requirements established in the Implementing the Recommendations of the 9/11 Commission Act (Pub. L. 110-53, 121 Stat. 266, 478, Aug. 3, 2007) (9/11 Act), TSA is developing a system to screen 50 percent of cargo transported aboard passenger aircraft by February 2009 and 100 percent of such cargo by August 2010.

In accordance with air cargo regulations issued in 2006, 71 FR 30478 (May 26, 2006), TSA currently conducts security threat assessments on several categories of individuals. One category consists of certain individuals who have, or are applying for, unescorted access to air cargo. Another category consists of individuals who are a sole proprietor, general partner, officer or director of an Indirect Air Carrier (IAC) or an applicant to be an IAC. An additional category consists of individuals who, in addition to having unescorted access to cargo, also have responsibilities for screening cargo under 49 CFR parts 1544, 1546 and 1548. The collection of PII from these individuals was described in an Air Cargo Security Requirements PIA dated April 14, 2006.

To meet the 9/11 Act requirements, TSA is establishing a new voluntary CCSP under which TSA will certify facilities to screen cargo intended for transport on a passenger aircraft. Under this program, TSA-approved validation firms will be used to assess the security of each certified cargo screening facility (CCSF). As part of the CCSP, TSA will collect personal data from specified CCSF personnel and validation firm personnel, as described below.

Reason for the PIA Update

This PIA Update discusses the expanded set of PII necessary to process the STAs for the population of individuals discussed in the April 14, 2006 PIA. It also provides express notice to all individuals in the CCSP who are required to undergo an STA. Additionally, the PIA Update provides notice of revised data retention and redress policies applicable to all populations covered by TSA's air cargo security programs.

Unless otherwise noted, the information provided in the April 14, 2006 PIA remains in effect for all populations required to submit STA data under TSA's air cargo security programs. This PIA Update provides a summary of key sections of the April 14, 2006 PIA for ease of understanding by the CCSP population. Individuals are encouraged to read both the April 14, 2006 PIA and this PIA Update to have a complete understanding of TSA's privacy analysis of its PII collection activities for its air cargo security programs.

Privacy Impact Analysis

The System and the Information Collected and Stored within the System

Expanded Data –In addition to the data elements discussed in the April 14, 2006 PIA necessary for completing the STA, TSA will now require all individuals requesting an STA to submit their daytime telephone numbers and the names, addresses, and telephone numbers of the individuals' employers. This information is very helpful in the adjudication process if the applicant has failed to submit complete information or TSA needs additional information to complete the STA. Adjudicators often contact applicants by telephone with questions, and this typically saves time and expense for the applicant and TSA by facilitating immediate resolution of the issues.

For non-U.S. citizens who do not have an Alien Registration Number, TSA will collect the Form I-94 Arrival/Departure Number. For non-U.S. citizens, TSA must have either the Alien Registration Number or the Form I-94 number to identify the immigration status of a non-citizen, including whether a non-citizen is working in the U.S. beyond his or her authorized stay. This collection allows for more accurate determinations of lawful immigration status, reducing potential risk to the air cargo supply chain and improving the accuracy of the STA result.

New Program – Under the CCSP, TSA will require STAs for the following categories of individuals (CCSP Individuals):

- CCSP individuals with unescorted access to screened cargo.
- CCSP individuals performing or supervising screening.
- The senior manager or representative in control of the operations of a CCSF.
- Employees of validation firms supervising, performing, or assisting in validations.
- Security coordinators and their alternates of certified cargo screening facilities and validation firms.

These individuals play important roles in securing cargo transported on passenger aircraft. TSA will conduct an STA to determine whether the individuals are ineligible or may pose a threat to national or transportation security before allowing them to perform specified functions under the CCSP.

TSA will use the STA Tool, a secure web tool, to facilitate the collection, processing, and retention of the following information on all CCSP individuals on whom an STA is conducted:

1. Legal name, including first, middle, and last; any applicable suffix; and any other names used.

2. Current mailing address, including residential address if different than current mailing address, and all other residential addresses for the previous five years and email address, if applicable.
3. Gender.
4. Date and place of birth.
5. Social security number (SSN)[1].
6. Citizenship status and date of naturalization if the individual is a naturalized citizen of the United States.
7. Alien registration number or Form I-94 Arrival/Departure Number, if the individual is not a U.S. citizen.
8. Daytime phone number.
9. Name, address, and telephone number of the individual's employer.

In addition to the information listed above, TSA may collect and maintain information that an individual chooses to submit in connection with an appeal of a TSA determination, such as letters from a prosecutor, documents from a board of pardons, police documents, or other relevant documents.

In some cases, an individual may have successfully completed an STA conducted by another government agency, and this STA may be acceptable for the air cargo program. If the individual asserts completion of a comparable threat assessment in lieu of a new security threat assessment, the individual should submit the name of the program for which the comparable threat assessment was conducted and the date on which it was completed.

In the future, TSA may exercise its authority under 49 CFR part 1540 to require fingerprint-based criminal history records checks (CHRC) for individuals who work for CCSFs or TSA-approved validator's, and who have responsibility to screen cargo. TSA may require CHRCs to identify whether the individual has been convicted of a disqualifying crime, such as interference with air navigation, aircraft piracy, espionage, or any of the other enumerated crimes listed at 49 CFR § 1544.229(d). If TSA exercises this authority, individuals will have to provide fingerprints and associated biographic data to TSA to conduct CHRCs. Fingerprints may also be shared within the Department of Homeland Security (DHS) using DHS's United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Automated Biometric Identification System (IDENT) system in order to perform enhanced immigration checks.

Uses of the System and the Information

The uses of the system and information in support of the CCSP are consistent with the processes discussed in more detail in the April 14, 2006 PIA. The STA information is being collected to carry out TSA's statutory mandate to secure the air cargo supply chain. CCSF personnel and TSA-approved validators are critical links in securing cargo transported in aircraft. TSA uses the information provided to conduct STAs on TSA-approved validators and on employees and agents of CCSFs to determine whether they pose a security risk. STAs consist of checks of Federal terrorism, law enforcement, and immigration databases. If the CHRC requirement is implemented, TSA may enroll fingerprint and associated biographic data within DHS's IDENT system. Finally, TSA may verify the accuracy of SSN with the Social Security Administration, with the consent of the individual.

[1]Although provision of one's social security number is voluntary, failure to provide a social security number may result in delays or prevent completion of the security threat assessment.

Individual information may be shared with third parties during the course of an STA or adjudication of a waiver or appeal, to the extent necessary to obtain information pertinent to the assessment or adjudication of the applicant or in accordance with the routine uses identified in the system of records notice for the Transportation Security Threat Assessment System (T-STAS) DHS/TSA-002, November 5, 2005, 70 FR 67731 System of Records Notice (SORN).

Retention

The following is an update to the records retention discussion provided in the April 14, 2006 PIA and applies to all populations on whom an STA is conducted. Since that date, the National Archives and Records Administration (NARA) has approved TSA's schedule.

TSA will retain the information in accordance with the National Archives and Records Administration (NARA) records schedule approved March 8, 2007, Transportation Threat Assessment and Credentialing. The approved NARA schedule contains the following dispositions:

- TSA will delete or destroy information contained in the Subject Database System one year after it is notified by the airport that the individual's credential or access privilege, which was granted based upon the STA, is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are later determined not to pose a threat to transportation or national security, retained information will be destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer.
- Information contained in the Subject Database System on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted or destroyed ninety-nine years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

Internal Sharing and Disclosure

As discussed in more detail in the April 14, 2006 PIA, information will be shared within DHS with those officials and employees who have a need for the information in the performance of their duties. In the ordinary course, information will be shared within TSA with the Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Intelligence in the event of a match or possible match, Office of Chief Counsel for enforcement action or other investigation, Office of Security Operations for operational response and compliance inspection, and the Office of Transportation Sector Network Management (TSNM) for program management. Information may also be shared with the TSA Office of Civil Rights and Liberties, TSA Privacy Office, TSA Ombudsman, and TSA Legislative Affairs to respond to complaints or inquiries. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. It is also expected that information will be shared with Immigration and Customs Enforcement (ICE) and U.S. Citizenship & Immigration Service (USCIS) for immigration issues.

TSA will also share fingerprints and associated biographic information with DHS's IDENT system as part of the STA. Further information about IDENT can be found in the IDENT PIA publicly available on the DHS website.

TSA minimizes the potential privacy risks that personal information may be disclosed to unauthorized individuals using a set of layered privacy safeguards that include physical, technical, and administrative

controls to protect personal information in the automated system, appropriate to its level of sensitivity. Privacy risks associated with sharing information with IDENT are mitigated by sharing in accordance with the Privacy Act, T-STAS SORN, and by the system user limitations within the IDENT system identified in the IDENT PIA.[2]

External Sharing and Disclosure

As discussed in more detail in the April 14, 2006 PIA, the information will be shared with the FBI for individuals for whom TSA conducts criminal history records checks, and with the Terrorist Screening Center to resolve potential watch list matches. TSA also may share the information it receives with Federal, State, or local law enforcement, immigration, or intelligence agencies or other organizations, in accordance with the routine uses identified in the applicable T-STAS SORN.

TSA may also share information with the Social Security Administration (SSA) to confirm the validity of SSN provided by the individual. Individuals will be asked to expressly authorize SSA to confirm the validity of the SSN.

TSA will share the final results of all STAs and CHRCs with the individual's employer.

Notice

General Notice to the public is provided by this PIA Update.

TSA will provide a written notice under 5 U.S.C. 552a (e)(3) (Privacy Act) to individuals at the time the individual's information is collected.

Concurrent with the STA submission individuals must sign a statement acknowledging that TSA may notify the individual's operator if TSA or other law enforcement agency becomes aware that the applicant poses an imminent security threat.

Individual Access, Redress, and Correction

The following changes apply to all populations on whom an STA is conducted under TSA's air cargo security programs. If TSA determines that the individual is not eligible or poses a security threat, TSA will issue an Initial Determination of Threat Assessment (IDTA) to the individual. The determination includes a statement that explains why TSA believes the individual is not eligible or may pose a security threat and the process by which the individual may appeal the determination. TSA is expanding the timeframe in which all individuals may appeal an IDTA from 30 to 60 days. This change was made to accommodate the needs of certain types of workers for whom the 30-day timeframe is inadequate for submitting appeal information to TSA.

The process for responding to IDTAs is the same for all covered individuals and is detailed in the April 14, 2006 PIA. If TSA determines that the individual poses an imminent threat to transportation or national security, or of terrorism, TSA issues an IDTA and Immediate Revocation to the individual and may notify the operator.

---

[2] http://www.dhs.gov/xabout/structure/editorial_0338.shtm

The processes for Individual Access, Redress and Correction are consistent with practices discussed in the April 14, 2006 PIA and create no new privacy risks.

Technology and Security

STA Tool is a web-based tool facilitating the collection and processing of all CCSP STA data and is currently in the Development phase of the TSA Systems Development LifeCycle (SDLC). The system is designed to protect the information it manages through implementation of comprehensive security controls.

Consistent with the information security practices discussed in the April 14, 2006 PIA, TSA will secure personal information in the STA Tool against unauthorized use through a layered security approach involving procedural and information security safeguards. The data will be encrypted using National Institute of Science and Technology (NIST) standards and industry best practices when being transferred between secure workstations. Federal Information Security Management Act (FISMA) certification and accreditation will be prepared once the software programs are developed. Only TSA employees and contractors with proper security credentials and passwords, and a need to know in order to fulfill their duties associated with conducting security threat assessments, will have access to this information. Moreover, all TSA and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data.

Specific privacy safeguards can be categorized by the following means:

- Technical limitations on, and tracking of, data access and use;
- Use of secure telecommunications techniques; and
- Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

- The Privacy Act of 1974, as amended (5 U.S.C. 552a), which requires Federal agencies to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of information protected by the Act.

- Federal Information Security Management Act of 2002 (Pub. L. 107-347) which establishes minimum security practices for Federal security systems.

Responsible Official

Victor Parker
Branch Chief, Policy and Strategic Planning
Air Cargo Security
Transportation Security Administration
Department of Homeland Security

Approval Signature Page

Original singed and on file with the DHS Privacy Office

John W. Kropf
Deputy Chief Privacy Officer
Department of Homeland Security